Amendments to the Claims:

1.-10. (canceled)

11. (currently amended) A method for setting limit values of an access control for limiting traffic transmission in a communication network, wherein the communication network comprises a plurality of pairs of marginal nodes at margins of the network, each pair associated with a set of possible paths comprising internal nodes and internal links leading through the communication network which run between each pair and through ~~between~~ which the transmission occurs along a possible path without explicit path reservation, ~~and the limit values of the access control are limit values regarding the pairs,~~ the method comprising ~~the following steps~~:

for each pair of marginal nodes in the communication network,

(a) ~~setting~~ initializing the limit values ~~such that probabilities for each of the pairs related to not approving the transmission between the marginal nodes of the pair, without explicit path reservation, are~~ to a predetermined initial low value such that substantially the same high blocking probabilities exist for all pairs of marginal nodes~~,~~ ~~and such that~~ thereby avoiding an overload situation in the communication network ~~does not occur~~;

(b) iteratively increasing the limit values ~~to~~ until ~~a minimum value at which~~ an overload situation ~~starts to occur~~ is identified at one of the internal links, ~~such that the probabilities are substantially the same~~;

(c) determining which of the pairs of marginal nodes contributed to the overload situation at the identified internal link by determining which of the pairs have possible paths that run through the identified link; ~~and~~

(d) ~~updating~~ setting the limit value ~~regarding at least one of~~for the pairs of marginal nodes that contributed to~~, between which a transmission occurs causing~~ the overload situation ~~, by setting the~~to a limit value ~~to the minimum value~~of an immediately prior iteration;

(e) repeating steps (b) through (d) until limit values are set for all pairs of marginal nodes as overload situations are identified at other internal links.

thereby providing access control at the margins of the network by setting limit values for each pair of marginal nodes based on its respective contribution to overload situations occurring at internal links in the set of possible paths for that pair of marginal nodes.

12. (currently amended) The method in accordance with claim 11, wherein the blocking probabilities are related to not approving the transmission between the marginal nodes of the pairs ~~are blocking probabilities related to blocking the transmission between the marginal nodes of the pairs~~.

13. (previously presented) The method in accordance with claim 11, wherein the marginal nodes include nodes of the network representing sources or sinks of traffic of the network.

14. (previously presented) The method in accordance with claim 11, wherein the marginal nodes are specified by ingress nodes and egress nodes of the network.

15. (previously presented) The method in accordance with claim 14, wherein the plurality of the pairs comprises all pairs of the network consisting of an ingress node and an egress node in each case.

16. (previously presented) The method in accordance with claim 11, wherein the overload situation is produced when in a scenario of high traffic load, in which the limit values for the access controls are still adhered to, a threshold value is exceeded on a link for the traffic transmitted over the link.

17. (previously presented) The method according to claim 16, wherein the threshold value for the traffic transmitted over the link is assigned to the link such that in case of failure of the link, the traffic allowed within the framework of the access controls does not represent any overload.

18 - 21. (cancelled).

22. (previously presented) The method in accordance with claim 11, further comprising:

making access checks for all the traffic of a class of service.

23. (previously presented) The method in accordance with claim 22, wherein the access checks relate to an approval or rejection of individual flows.

24. (previously presented) A network node with means for executing the method in accordance with claim 11.

25. (previously presented) The network node according to claim 24, wherein the network node is a marginal node of the network.

26. (currently amended) A method for setting limit values of an access control for limiting traffic transmission in a packet-switched communication network comprising a plurality of marginal nodes and a plurality of internal nodes, the method comprising:

(a) identifying all pairs of marginal nodes in the network, wherein each pair of marginal nodes is identified as an origination and destination node of a given transmission in a given direction within the network, and not an intermediate internal node in the given transmission, and is associated with a set of possible paths comprising intermediate internal nodes and internal links leading through the network between each pair and through which traffic flows along a possible path without explicit path reservation;

(b) using a traffic model to set an initially low traffic threshold value for each pair of marginal nodes ~~without explicit path reservation~~ so that substantially the same high blocking probabilities ~~are substantially the same for~~exist each pair of marginal nodes;

(c) operating the network with communications traffic;

(d) iteratively increasing the threshold values of all pairs of marginal nodes ~~step-by-step~~ until congestion ~~occurs~~ is detected on an internal link of at least one pair of marginal nodes;

(e) reducing the threshold value ~~on the at least one pair~~ for all pairs of marginal nodes that contributed to the detected congestion to the threshold value at the iterative step before the detected congestion ~~occurred~~, wherein the pairs of marginal nodes that contributed to the detected congestion comprise those pairs of marginal nodes with possible paths that run through the internal link which is causing the congestion; and

(f) repeating steps (d) though (e) ~~from the increasing step~~ on the remaining pairs of marginal nodes until each of the pairs of marginal nodes has ~~reached a respective congestion and then~~ its threshold value ~~has been~~ reduced in accordance with its contribution to congestion ~~to the step before the respective congestion occurred~~;

whereby traffic throughput of all marginal pairs of the network is optimized.

27. (previously presented) The method according to claim 26, wherein each pair of marginal nodes is defined as an ingress node and an egress node, or an ingress node into the network and an addressee node of the given transmission within the network, or a transmitter node of the given transmission within the network and an egress node from the network, regardless of traffic path and internal nodes for routing the given transmission between the pair of marginal nodes.

28. (currently amended) A method for setting limit values of an access control for limiting traffic transmission in a packet-switched communication network comprising a plurality of marginal nodes and a plurality of internal nodes, the method comprising:

(a) identifying all pairs of marginal nodes in the network, wherein a pair of marginal nodes is defined as a starting and ending point of a given transmission in a given direction in the network, including an ingress node and an egress node, or an ingress node and an addressee node of the given transmission, or a transmitter node of the given transmission and an egress node, regardless of a path of the given transmission between the pair of marginal nodes and wherein each pair is associated with a set of possible paths comprising intermediate internal nodes and internal links leading through the network between each pair and through which traffic flows along a possible path without explicit path reservation;

(b) estimating a traffic blocking probability for each pair of marginal nodes using a traffic model;

(c) setting a traffic limit value for each pair of marginal nodes based on the traffic model low enough so that no overload situation occurs in the network, and wherein the high initial blocking probability for each of the pairs of marginal nodes is substantially the same;

(d) operating the network with communications traffic;

(e) raising the limit values on all of the marginal nodes, step by step, until a first overload occurs on an internal link of one or more pairs of overloaded marginal nodes, wherein the pairs of overloaded marginal nodes comprise those pairs of marginal nodes with possible paths that run through the internal link which is causing the congestion; and

(f) reducing the limit value on each of the overloaded marginal nodes to the limit value at the step prior to the first overload, and not reducing the limit value on the remaining non-overloaded pairs of marginal nodes.

29. (previously presented) The method in accordance with claim 28, further comprising:

raising the limit values of all of the remaining non-overloaded nodes, step by step, until a next overload occurs on one or more next pairs of overloaded marginal nodes; and

reducing the limit value on each of the next overloaded marginal nodes to the limit value at the step prior to the next overload, and not reducing the limit value on the remaining non-overloaded pairs of marginal nodes.

30. (previously presented) The method in accordance with claim 29, further comprising repeating the steps of claim 29 in order one or more times.